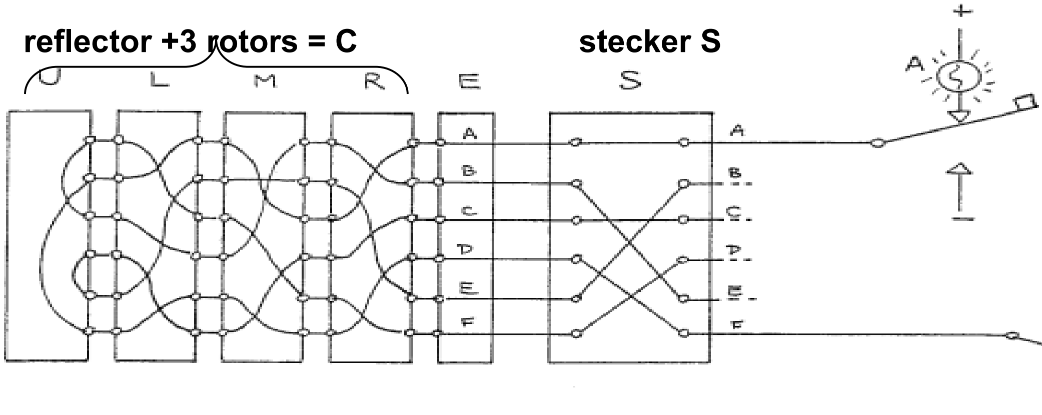
Understanding HOW Enigma Was Broken or How Mathematicians Won the WW2 [cf. UCL COMPGA18 course].

1. In 1920s a "commercial Enigma" machine was invented. Rotors rotate and each letter is encrypted by a different circuit of permuted wires. Yet it could be broken by paper and pencil. Unlike most countries German cipher machines was a lot stronger. Since 1930 Germany encrypted their communications with a "military Enigma" which is a LOT more complex. It differs by the introduction of the so called '**stecker'** [plug board] which increased the entropy of the key tremendously by some 47 extra bits (150 million million times) to about 76 bits.



2. For the next 10 years it was considered unbreakable and its details remained unknown at BP. To know the [secret] connections of one rotor was equivalent to having an additional secret of 88 bits. However the same rotors remained in use for decades. The French had a spy H. in the German security service. This spy has not supplied an Enigma machine however he gave them a manual which contained examples settings+plaintext+ciphertext.
3. This allowed Polish mathematicians to recover the wirings of the rotors [by advanced mathematics / factoring permutations]. In 1932-1938 messages were decrypted in Poland due to major mistakes in setup procedures.
4. In Dec 1938 the setup method was changed and the Poles invented 2 new attacks: **Rejewski**'s bombe which and Zygalski sheets method. All the knowledge [and machines] were given to allies [France and Britain] in July 1939.
5. **Zygalski** method was already very expensive and actually it was only fully implemented by Jeffreys at Bletchley Park a year later, and allowed the Poles+French+UK to decrypt Enigma traffic until May 1940 [invasion of France].
6. In late 1939 **Alan Turing** has started developing a new [more general and a lot more expensive] attack which would decrypt Enigma messages ignoring weak setup, anticipating that one day Polish attacks will stop working.
7. The cost of breaking Enigma became huge, say a price of 100 extra war planes and **Churchill** personally made sure that code breakers obtained money required. First Bombe by Turing [just before May 1940] didn't work well.
8. Another mathematician **Gordon Welchman** has invented a so called diagonal board, a tremendous improvement.
9. Overall we call it the **Turing–Welchman Bombe Attack** on Enigma. It allows to totally ELIMINATE the stecker and find the 3 rotor positions [previous attacks assumed weak setup/init or less connections in the stecker].

The attack works in 3 stages [it will be explained during our visit and we will see a working real-life demo in block B]:

1. First code breakers need to guess a **crib**, part of the plaintext, for example NOTHINGTOREPORT.
2. They compared plaintext to many encrypted messages. Enigma has one terrible weakness: no letter would encrypt to itself. Consequently, most of the time it was possible to reject a given alignment of the crib.
3. Codebreakers could therefore guess a plausible alignment which could be correct.
4. From this they created a so called **menu**. A graph in which pairs of letters are connected, say G encrypts to P.
5. Turing approach exploits short cycles in this graph. For example imagine we have a simple cycle of length 3 G=>P=>A=>G [length 2 would be broken by earlier Polish attacks, Turing attack was for cycles of any length].
6. Turing focused on the possibility to obtain the same G again. If we connect several Enigmas in a closed loop [just following our cycle] and if we connect wire G to a battery, the current will come out at same letter G.
7. A cycle in the 'menu' implies **a fixed point** for a certain sequence of full encryptions. For example **P**(G)=G where **P** is a combination of full Enigmas with settings which differ by a few steps in time, e.g. $\mathbf{t=t_0}$+2 in first Enigma.
8. Let **S** be the permutation of the stecker and let $\mathbf{C_2}$, $\mathbf{C_5}$ and $\mathbf{C_8}$ are the combined permutations of going through 3 rotors and back in Enigma at clocks 2, 5 and 8. We have $\mathbf{P = S^{-1}.C_2.S.S^{-1}.C_5.S.S^{-1}.C_8.S}$ [read right to left].
9. So G = $\mathbf{S^{-1}.C_2.S.S^{-1}.C_5.S.S^{-1}.C_8.S.}$G which simplifies to **S.**G = $\mathbf{C_2.C_5.C_8.S.}$G; **S(G)** is a fixed point for $\mathbf{C_2.C_5.C_8}$!
10. This permutation $\mathbf{C_2.C_5.C_8}$ is implemented through composition of 3 so called Letchworth Enigmas [which had separated inputs and output allowing arbitrary combinations to be build]. Three sets of 3 drums on the bombe are connected at the back of the bombe through 26-wire red cables 'spaghetti'. Diagonal board=>extra connections.
11. A nice trick is just to input some random letter say A to this circuit $\mathbf{C_2.C_5.C_8}$ connected as an 'infinite' loop.
12. Most of the time the machine actually tries totally wrong settings. Then A is not a fixed point for $\mathbf{C_2.C_5.C_8}$.
13. So current comes out at another letter, then because we have a closed loop, it goes inside again. Typically all 26 letters are 'live'. This is clearly a wrong setting. Frequently we have no fixed point at all, 26 wires are active, and all 'fast' rotors in the machine turn to try the next setting [search actually done backwards **t**=ZZZ+2..AAA+2].
14. Now if $\mathbf{C_2.C_5.C_8}$ has a fixed point D, the current will reach 25 wires EXCEPT D. If this happens the machine stops. We should now think that **S(G)=D.** This is if the 3 rotors are at correct positions. Then recover two full S on the checking machine. Typically it will have 10 swaps and 6 fixed points. If not, re-start the bombe again.
15. Overall during WW2 Britain have recovered 25,000 keys and decrypted 2M messages shortening war by 2 years.